

RECEIVED
CENTRAL FAX CENTER

DEC 07 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Lotspiech)	Art Unit: 2137
Serial No.: 09/771,239)	Examiner: Davis
Filed: January 26, 2001)	ARC: 920010006US1
For: METHOD FOR TRACING TRAITOR RECEIVERS IN A BROADCAST ENCRYPTION SYSTEM)	December 6, 2004 750 B STREET, Suite 3120 San Diego, CA 92101

DECLARATION UNDER RULE 131

Commissioner of Patents and Trademarks
Washington, DC 20231

Dear Sir:

We, the below-named inventors of the above-captioned application, declare as follows:

As evidenced by the enclosed relevant pages from the IBM Invention Disclosure form dated as being created on September 14, 2000 and modified on December 7, 2000 (cover page of enclosed disclosure), we conceived of the present invention at least prior to January 1, 2001. Specifically, using the limitations of Claim 4 as an example and referring to the enclosed document, the inventors conceived of a method for identifying or disabling at least one traitor receiver with an associated unique, compromised decryption key in a broadcast encryption system (first content page of disclosure, first paragraph, discussing broadcast to users that have their own keys, which may "leak" if a device is a traitor); receiving a set of subsets derived from a tree defining leaves, each leaf representing a respective receiver (second content page, discussing "complete subtree" and "subtree difference" methods; bottom of third page continuing to top of fourth page, discussing partitioning subsets only if it

1003-112-855

CASE NO.: ARC920010006US1
Serial No.: 09/771,239
December 6, 2004
Page 2

PATENT
Filed: January 26, 2001

contains a traitor and continuing to partition until a subset contains only a single traitor, which can then be revoked); identifying at least one traitor subset from the set of subsets as containing at least one leaf representing a traitor receiver, (see above), using the traitor subset, identifying or disabling the traitor receiver (fourth page, first bullet); and determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets, fourth page, second bullet. Also, the specific method may include encoding plural subsets of the set of subsets with a false key, bottom of fifth page continuing to sixth page. The disclosure also teaches several additional features of one or more dependent claims as shown in the various pages enclosed herewith.

We declare that the inventors and assignee were diligent in reducing the invention to practice at least from a time prior to January 1, 2001 at least to the present filing date. Specifically, we declare that the enclosed invention disclosure prior to January 1, 2001 to IBM Intellectual Property Department, which then diligently processed the application for disclosure to outside counsel in December 2000. A first draft application was prepared for inventor review on January 5, 2001, which was then diligently reviewed for filing on January 26, 2001 within the usual course of IBM business in filing patent applications.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United State Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

1033-722AFY

FROM ROGITZ 619 338 8078
JAN-1-1999 12:15P FROM:

(TUE) DEC 7 2004 15:53/ST. 15:50/No. 6833031378 P 15
TO: 16193388078 P: 4-4

CASE NO.: ARC920010006(US)
Serial No.: 09/771,239
December 6, 2004
Page 3


PATENT
Filed: January 26, 2001

BY: Dalit Naor
date:


Jeff Lotspiech


Nimcon (Moni) Naur

Respectfully submitted,


John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JI.R:jg

1051-122, N18